UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/989,806	11/20/2001	Tao Haukka	4925-163	1608

7590 03/22/2005

COHEN, PONTANI, LIEBERMAN & PAVANE
Suite 1210
551 Fifth Avenue
New York, NY 10176

EXAMINER	
CHAI, LONGBIT	

ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 03/22/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/989,806	HAUKKA ET AL.	
	Examiner	Art Unit	
	Longbit Chai	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *07 October 2002*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☐ Claim(s) _____ is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-74* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *07 October 2002* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *11/20/2001*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Priority

1. No claim for priority has been made in this application.

The effective filing date for the subject matter defined in the pending claims in this application is 11/20/2001.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraph of 35 U.S.C. 102 that forms the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

2. Claims 1, 21 – 24, 44 – 47, 61 – 64 and 73 – 74 are rejected under 35 U.S.C. 102(e) as being anticipated by Vatanen (Patent Number: 2003/0078058).

As per claim 1, 24, 47 and 64, Vatanen teaches a method for incorporating confidentiality protection in a message transmitted between a user equipment and a network element in a communication network, wherein the message requires a sender identification and the sender of the message is one of the user equipment and the network element, the method comprising the steps of:

(a) assigning a temporary identity index for the sender of the message at each of the user equipment and the network element including performing an algorithm for generating the temporary identity index using public information which identifies the sender of the message as an input to the algorithm (Vatanen: see for example, Para [0005] Line 6 – 9, Para [0021]: The MUI (pidKey) is interpreted as the temporary identity index and the given name is interpreted as the public information); and

(b) adding a header including the temporary identity index to the message to identify the sender of the message prior to transmission of the message between the user equipment and the network element (Vatanen: see for example, Para [0021] Line 1 – 3 and Para [0021] Line 12 – 14 & Figure 1).

As per claim 21, 44, 61 and 73, Vatanen teaches the claimed invention as described above (see claim 1, 24, 47 and 64 respectively). Vatanen further teaches said user equipment is a mobile phone (Vatanen: see for example, Para [0018] Line 9).

As per claim 22, 45 and 62, Vatanen teaches the claimed invention as described above (see claim 1, 24 and 47 respectively). Vatanen further the algorithm is known to both the user equipment and the network element and said step (a) includes separately performing the algorithm at each of the user equipment and the network element (Vatanen: see for example, Para [0011] Line 6 – 10 and Para [0002]).

As per claim 23, 46, 63 and 74, Vatanen teaches the claimed invention as described above (see claim 1, 24, 47 and 64 respectively). Vatanen further teaches said step (a) includes performing the algorithm at the communication network and assigning the temporary identity index to the user equipment and the network element (Vatanen: see for example, Para [0002] and [0009] & Figure 1).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> A person shall be entitled to a patent unless –
>
> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 2, 25, 48, 65 and 66 are rejected under 35 U.S.C. 103(a) as being unpatentable over Vatanen (Patent Number: 2003/0078058).

As per claim 2, 25, 48, 65 and 66, Vatanen teaches the claimed invention as described above (see claim 1, 24, 47, 64 and 65 respectively). Vatanen further teaches in said step (a), performing an algorithm includes performing a hash function using a private key and the public information as inputs to generate the temporary identity index (Vatanen: see for example, Para [0021]: Vatanen teaches the hash function key is a public signing key. Vatanen does not disclose expressly the hash function key is a

private key. However, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to modify Vatanen to use a private key for hash function because both public signing key and private key (i.e. public-private key pair) are security keys and hash function using a security key are well known in the art).

4. Claims 3, 4, 9, 16, 26, 27, 32, 39, 49, 52 and 67 are rejected under 35 U.S.C. 103(a) as being unpatentable over Vatanen (Patent Number: 2003/0078058), and in view of 3G-TS-33.203 ("3GPP Access Security for IP-Based Serveices").

As per claim 3 and 26, Vatanen teaches the claimed invention as described above (see claim 1 and 25 respectively). Vatanen does not disclose expressly the public information used in said step (a) is an internet protocol multimedia public identity of the user equipment.

3G-TS-33.203 teaches the public information used in said step (a) is an internet protocol multimedia public identity of the user equipment (3G-TS-33.203: see for example, Sec. 3.3 – IMPU (Internet Multimedia Public Identity)).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of 3G-TS-33.203 within the system of Vatanen because (a) Vatanen teaches signing / encrypting of the sender identity and the integrity of a message in he Global System for Mobile Communications telecommunication networks (Vatanen: see for example, Para [0002] and [0005]) and (b) 3G-TS-33.203 teaches enhancing the security features for secure access to the

Internet Multimedia subsystem for the 3G mobile telecommunication system (3G-TS-33.203: see for example, Scope section).

As per claim 4, 27 and 49, Vatanen in view of 3G-TS-33.203 teaches the claimed invention as described above (see claim 1, 24 and 47 respectively). Vatanen does not disclose expressly registering the user equipment with the visiting network before said step (a).

3G-TS-33.102 teaches registering the user equipment with the visiting network before said step (a) (3G-TS-33.203: see for example, Section 6.1.1 and Sec. 3.3 – IMPU (Internet Multimedia Public Identity): Registration of an IM-subscriber provides the public identity, and thereby registration must be proceeded first in order to perform the hash function and further assign a temporary identity index for the sender of the message).

See the same rationale applied herein as above in rejecting claim 3.

As per claim 9, 32, 52 and 67, Vatanen teaches the claimed invention as described above (see claim 1, 24, 47 and 64 respectively). Vatanen does not disclose expressly the message is a session initiation protocol message.

3G-TS-33.203 teaches the message is a session initiation protocol message (3G-TS-33.203: see for example, section of Scope). See the same rationale applied herein as above in rejecting claim 3.

Vatanen in view of 3G-TS-33.203 further teaches generating the session initiation protocol message and encrypting the session initiation protocol message before performing said step (b) (Vatanen: see for example, Figure 1 & Para [0012] Line 1 – 6); and wherein said step (b) includes adding another line including the temporary identity index before the encrypted session initiation protocol message (Vatanen: see for example, Para [0021] Line 12 – 13).

As per claim 16 and 39, Vatanen in view of 3G-TS-33.203 teaches the claimed invention as described above (see claim 9 and 32 respectively). Vatanen further teaches performing an integrity algorithm for the entire session initiation protocol message to calculate a code and adding an integrity header to the session initiation protocol message indicating the code (Vatanen: see for example, Para [0018] and Figure 1).

5. Claims 5 – 8, 28 – 31, 50 and 51 are rejected under 35 U.S.C. 103(a) as being unpatentable over Vatanen (Patent Number: 2003/0078058), and in view of 3G-TS-33.203 (3GPP Access Security for IP-Based Serveices), and in view of 3G-TS-33.102 ("3GPP Security Architecture").

As per claim 5, 28 and 50, Vatanen in view of 3G-TS-33.203 teaches the claimed invention as described above (see claim 4, 27 and 49 respectively). Vatanen in view of 3G-TS-33.203 does not disclose expressly registering comprises sending, by the user

equipment, a registration message to the network element, and retrieving, by the visiting network, the private key from a home network of the user equipment.

3G-TS-33.102 teaches registering comprises sending, by the user equipment, a registration message to the network element, and retrieving, by the visiting network, the private key from a home network of the user equipment (3G-TS-33.102: see for example, Page 17 Figure 4. Both of CK (Ciphering Key) and IK (Integrity Key) are considered as the private keys).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of 3G-TS-33.102 within the system of Vatanen in view of 3G-TS-33.203 because 3G-TS-33.102 further enhancing the security by providing a mutual authentication mechanism between the user and the network showing the knowledge of a secret key (3G-TS-33.102: see for example, Page 16 Sec. 6.3).

As per claim 6 and 29, Vatanen in view of 3G-TS-33.203 teaches the claimed invention as described above (see claim 5 and 28 respectively). 3G-TS-33.102 further teaches the user equipment is authenticated after the network element retrieves the private key from the home network (3G-TS-33.102: see for example, Page 16 Sec. 6.3).

As per claim 7, 30 and 51, Vatanen in view of 3G-TS-33.203 and 3G-TS-33.102 teaches the claimed invention as described above (see claim 5, 28 and 50 respectively). 3G-TS-33.102 further teaches the private key comprises one of a ciphering key and an

integrity key (3G-TS-33.102: see for example, Page 17 Figure 4. Both of CK (Ciphering Key) and IK (Integrity Key) are considered as the private keys).

As per claim 8 and 31, Vatanen in view of 3G-TS-33.203 and 3G-TS-33.102 teaches the claimed invention as described above (see claim 5 and 28 respectively). Vatanen further teaches determining an encryption algorithm and saving the private key, the encryption algorithm, and the temporary identity index in a memory in the visiting network (Vatanen: see for example, Para [0021] Line 9 – 11).

6. Claims 10 – 15, 17 – 20, 33 – 38, 40 – 43, 53 – 60 and 68 – 72 are rejected under 35 U.S.C. 103(a) as being unpatentable over Vatanen (Patent Number: 2003/0078058), and in view of 3G-TS-33.203 (3GPP Access Security for IP-Based Serveices), and in view of Moyer (Patent Number:2002/0103850).

As per claim 10, 33, 53 and 68, Vatanen in view of 3G-TS-33.203 teaches the claimed invention as described above (see claim 9, 32, 52 and 67 respectively). Vatanen in view of 3G-TS-33.203 does not disclose expressly adding a line before the encrypted session initiation protocol message including a request method of the session initiation protocol message.

Moyer teaches adding a line before the session initiation protocol message including a request method of the session initiation protocol message (Moyer: see for example, Para [0022] Line 8 – 11).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Moyer within the system of Vatanen in view of 3G-TS-33.203 because (a) Vatanen teaches signing / encrypting of the sender identity and the integrity of a message in he Global System for Mobile Communications telecommunication networks (Vatanen: see for example, Para [0002] and [0005]) and (b) Moyer teaches enhancing and improving the security features for secure access to the Internet Multimedia subsystem for the 3G mobile telecommunication system directed to SIP message (Moyer: see for example, Para [0028]).

Vatanen further teaches adding a line before the encrypted session initiation protocol message including a request method of the session initiation protocol message (Vatanen: see for example, Para [0012] Line 1 – 6).

As per claim 11, 34, 54 and 69, Vatanen in view of 3G-TS-33.203 teaches the claimed invention as described above (see claim 9, 32, 52 and 67 respectively). Vatanen in view of 3G-TS-33.203 does not disclose expressly the session initiation protocol message includes a line including the request method.

Moyer teaches the session initiation protocol message includes a line including the request method (Moyer: see for example, Para [0022] Line 8 – 11). See the same rationale applied herein as above in rejecting claim 10.

Vatanen further teaches session initiation protocol message includes a line including the request method that is encrypted with the session initiation protocol message (Vatanen: see for example, Para [0012] Line 9 – 11).

As per claim 12, 20, 35, 43, 55, 60, and 70, Vatanen in view of 3G-TS-33.203 teaches the claimed invention as described above (see claim 9, 19, 32, 42, 52, 59 and 67 respectively). Vatanen in view of 3G-TS-33.203 does not disclose expressly adding another line comprises adding a call-info header.

Moyer teaches adding another line comprises adding a call-info header (Moyer: see for example, Para [0022] Line 1 – 3). See the same rationale applied herein as above in rejecting claim 10.

Vatanen further teaches inserting the temporary identity index in the call-info header of the session initiation protocol message (Vatanen: see for example, Figure 1 & Para [0021]).

As per claim 13, 36, 56, 71, Vatanen in view of 3G-TS-33.203 and Moyer teaches the claimed invention as described above (see claim 12, 35, 55 and 70 respectively). Vatanen further teaches performing an integrity algorithm for the entire session initiation protocol message to calculate a code and adding an integrity header to the session initiation protocol message indicating the code (Vatanen: see for example, Para [0018] Line 12 – 17).

As per claim 14, 17, 37, 40 and 57, Vatanen in view of 3G-TS-33.203 and Moyer teaches the claimed invention as described above (see claim 13, 16, 36, 39 and 56 respectively). Vatanen further teaches said integrity algorithm comprises one of a

message authentication code integrity algorithm and a modification detection code integrity algorithm (Vatanen: see for example, Para [0018] Line 12).

As per claim 15, 18, 38, 41 and 58, Vatanen in view of 3G-TS-33.203 and Moyer teaches the claimed invention as described above (see claim 14, 17, 37, 40 and 56 respectively). Vatanen further teaches said integrity algorithm comprises MD5-MAC integrity algorithm (Vatanen: see for example, Para [0018] Line 12).

As per claim 19, 42, 59 and 72, Vatanen in view of 3G-TS-33.203 and Moyer teaches the claimed invention as described above (see claim 10, 33, 53 and 69 respectively). Moyer further teaches encrypting a uniform resource identifier for the sender and adding the encrypted uniform resource identifier to the line including the request method (Moyer: see for example, Para [0038]).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Longbit Chai whose telephone number is 571-272-3788. The examiner can normally be reached on Monday-Friday 8:00am-4:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Longbit Chai
Examiner
Art Unit 2131

LBC

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100